



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/577,449	05/24/2000	Scott C. Harris	SCH/BIOMETRICS	4716
23844	7590	01/02/2008	EXAMINER	
SCOTT C HARRIS P O BOX 927649 SAN DIEGO, CA 92192			SHIN, KYUNG H	
			ART UNIT	PAPER NUMBER
			2143	
			MAIL DATE	DELIVERY MODE
			01/02/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary

Application No.

09/577,449

Applicant(s)

HARRIS, SCOTT C.

Examiner

Kyung H. Shin

Art Unit

2143

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 12 June 2007.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 26-47 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 26-47 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- ☒ Notice of References Cited (PTO-892)
- ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date 9/5/07.
- ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____
- ☐ Notice of Informal Patent Application
- ☐ Other: _____

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 6/12/07 has been entered.
2. Application was filed on 5/24/2000, abandoned on 8/11/05 after Final action, and revived with RCE on 6/12/07. Claims **26 - 47** are pending. Claims **26 - 47** are new. Independent claims are **26, 37, 46**.
3. Applicant's arguments filed 6/12/2007 have been fully considered but are moot based on new grounds of rejection of **Hillhouse** (U.S. Patent No. **6,052,468**).

Claim Rejections - 35 USC § 112

4. The following is a quotation of the first paragraph of 35 U.S.C. 112:

The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.
5. Claims **26, 37, 46** are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter

which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. There is no disclosure for the limitation, "receiving information indicative of a code known to the user, as an entry into the computer". There is no disclosure of a code utilized as an input to gain entry a computer system.

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

7. Claims **26 - 31, 33 - 39, 41 - 47** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Bjorn** (U.S. Patent No. **6,035,398**) in view of **Hillhouse** (U.S. Patent No. **6,052,468**).

Regarding Claims 26, 37, Bjorn discloses a method of accessing files on a computer, comprising:

a) scanning a human body part to obtain information of said human body part that is indicative of at least one characteristic of the human body part; (see Bjorn col. 1, lines 39-42; col. 3, lines 26-30; col. 4, lines 4-7: generate biometric information

utilized for user authentication, characteristic of human body part (fingerprint))

- c) based on both said information indicative of said body part, and also on said code, using said computer for obtaining a cryptographic key which is used to enable a cryptographic operation which includes at least one of encryption or decryption of at least one file, on the computer; and using said cryptographic key to carry out at least one of encryption and/or decryption of at least one file on the computer. (see Bjorn col. 3, lines 32-34; col. 4, lines 17-19; col. 7, lines 32-34: generation of cryptographic key utilizing biometric features; col. 4, lines 30-46: generated key(s) utilized for encryption/decryption)

Bjorn does not specifically disclose whereby receiving information indicative of a code known to the user, as an entry into the computer.

However, Hillhouse discloses:

- b) receiving information indicative of a code known to the user, as an entry into the computer; (see Hillhouse col. 6, lines 45-52: cryptographic key generation from biometric information; col. 5, line 63 - col. 6, line 2: password, known to user, utilized for entry to computer system)

It would have been obvious to one of ordinary skill in the art to modify Bjorn as taught by Hillhouse to enable the capability whereby a code (password) is utilized for entry to a computer system. One of ordinary skill in the art would have been motivated to employ the teachings of Hillhouse in order to enable the capability for

secure management of cryptographic keys that does not impede portability of key databases. (see Hllhouse col. 3, lines 49-51: "*... It is presently known that a key database, once created, should never be decrypted, except during emergencies. This thinking prevents keys from becoming vulnerable by existing in their decrypted state. ... It would, however, be advantageous to enhance system security by providing secure key databases that do not impede portability of the key database. ...*")

Regarding Claims 27, 38, Bjorn discloses a method as in claim 26, wherein said scanning produces information which represents sufficient information about the human body part to render said information unique relative to other scanning of other body parts. (see Bjorn col. 3, lines 36-43: fingerprint information unique to fingerprint, comparison utilized for verification, (fingerprint uniqueness well known in the art))

Regarding Claims 28, 45, 47, Bjorn discloses a method as in claim 27, wherein said scanning comprises scanning a fingerprint to obtain information indicative of said fingerprint. (see Bjorn col. 1, lines 39-42; col. 4, lines 4-7; col. 3, lines 7-11: scan fingerprint utilizing sensor device)

Regarding Claim 29, Bjorn discloses a method as in claim 28, wherein said forming a cryptographic key comprises identifying a reference on the fingerprint, and using locations of features on the fingerprint relative to said reference to obtain said biometric

information. (see Bjorn col. 3, lines 32-34; col. 4, lines 17-19; col. 7, lines 32-34: generate cryptographic key from biometric information; col. 4, lines 13-24: utilize locations on fingerprint in cryptographic key generation)

Regarding Claim 30, Bjorn discloses a method as in claim 27, wherein said human body part is scanned to produce digital information that is indicative of an analog image, and further comprising converting aspects of the analog image into digital information indicative of said cryptographic key. (see Bjorn col. 1, lines 52-55: fingerprint image (analog image); col. 3, lines 32-34; col. 4, lines 17-19; col. 7, lines 32-34: image converted into cryptographic key)

Regarding Claims 31, 41, Bjorn discloses a method as in claim 26, wherein said forming a cryptographic key comprises first forming a first part of the cryptographic key using a first portion of the biometric information, subsequently and separately forming another part of the cryptographic key using another portion of the biometric information, and using both said one portion and said another portion of said biometric information together to form said cryptographic key. (see Bjorn col. 4, lines 13-24: cryptographic key generated utilizing some or all of biometric features information)

Regarding Claim 33, Bjorn discloses a method as in claim 31, wherein said forming comprises

- a) obtaining said first part of the cryptographic key from the one portion of the

biometric scan, (see Bjorn col. 4, lines 13-24: utilizing some or all of biometric features (curvature, ridge distance, etc.) for cryptographic key generation) and

- b) obtaining said another part of the cryptographic key from said another portion within the same biometric scan as the first portion, wherein said another portion is a different portion of the image than a first portion of image in which said one portion of the biometric scan is obtained. (see Bjorn col. 4, lines 13-24: utilize different portions (curvature, ridge distance, etc.) of fingerprint image for cryptographic key generation)

Regarding Claim 34, Bjorn discloses a method as in claim 31, wherein said forming comprises obtaining said first part of the cryptographic key from the one portion of the biometric scan, and getting said another part of the cryptographic key from said another portion within a different biometric scan from that scan that provides the first portion, wherein said another portion is based on a different image than a first image from which said one portion of the biometric scan is obtained. (see Bjorn col. 4, lines 13-24; col. 4, lines 4-7: utilizing some or all of biometric features (curvature, ridge distance, etc.) information to generate cryptographic key; different biometric scans (fingerprint scans, different fingers))

Regarding Claims 35, 44, Bjorn discloses a method as in claim 34, wherein said different biometric scan is a scan of a different body part than the part that provides said one portion. (see Bjorn col. 4, lines 4-7: different biometric body part, scan different

finger (different body part, see specification page 7))

Regarding Claim 36, Hillhouse discloses a method as in claim 26, wherein said biometric scan includes a retinal scan. (see Hillhouse col. 6, lines 45-52: cryptographic generation from biometric information; col. 6, lines 27-32: retinal scan, biometric scan)

It would have been obvious to one of ordinary skill in the art to modify Bjorn as taught by Hillhouse to enable the capability whereby a retinal scan as a biometric scan. One of ordinary skill in the art would have been motivated to employ the teachings of Hillhouse in order to enable the capability for secure management of cryptographic keys that does not impede portability of key databases. (see Hillhouse col. 3, lines 49-51)

Regarding Claim 39, Bjorn discloses a system as in claim 38, wherein said first scanning part includes a fingerprint scanner. (see Bjorn col. 3, lines 7-11: fingerprint sensor (scanner))

Regarding Claim 42, Bjorn discloses a system as in claim 41, wherein said routine forms said first portion and said different portion of the image than a first portion of image in which said one portion of the biometric scan is obtained. (see Bjorn col. 4, lines 13-24: different portions of image (curvature, ridge distance, etc.) utilized for cryptographic key generation)

Regarding Claim 43, Bjorn discloses a system as in claim 41, wherein said routine

forms said first portion and said another portion from different biometric scans, wherein said another portion is based on a different image than a first image from which said one portion of the biometric scan is obtained. (see Bjorn col. 4, lines 13-24: different portions of image (curvature, ridge distance, etc.) utilized for cryptographic key generation; col. 4, lines 4-7: different biometric body part, scan a different finger (see specification page 7))

Regarding Claim 46, Bjorn discloses a method, comprising:

- a) scanning a human body part to obtain first information therefrom that uniquely represents the scanned body part; (see Bjorn col. 3, lines 7-11; col. 4, lines 4-7: obtain fingerprint image, unique representation of body part)
- c) forming third information from one portion of said first information, and forming fourth information from another portion of said first information; (see Bjorn col. 4, lines 13-20: portions of biometric information utilized to generate cryptographic key) and
- d) obtaining a cryptographic key based on all of said second information, said third information, and said fourth information; (see Bjorn col. 3, lines 32-34; col. 4, lines 17-19; col. 7, lines 32-34: generation of cryptographic key utilizing biometric features (some or all of features)) and
- e) using said cryptographic key to carry out one of an encryption of information or a decryption of information on a computer. (see Bjorn col. 4, lines 30-46: keys utilized for encryption/decryption)

Bjorn does not specifically disclose whereby receiving second information indicative of a code known to the user.

However, Hillhouse discloses:

- b) receiving second information indicative of a code known to the user; (see Hillhouse col. 6, lines 45-52: cryptographic generation from biometric information; col. 5, line 63 - col. 6, line 2: password, known to user, utilized for entry to computer system)

It would have been obvious to one of ordinary skill in the art to modify Bjorn as taught by Hillhouse to enable the capability whereby a code (password) is utilized for entry to a computer system. One of ordinary skill in the art would have been motivated to employ the teachings of Hillhouse in order to enable the capability for secure management of cryptographic keys that does not impede portability of key databases. (see Hillhouse col. 3, lines 49-51)

8. Claims **32, 40** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Bjorn-Hillhouse** and further in view of **Takhar** (U.S. Patent No. **6,002,787**).

Regarding Claim 32, Bjorn discloses a method as in claim 27, wherein said forming uses said biometric information for a biometric authentication system. (see Bjorn col. 3, lines 32-34; col. 4, lines 17-19; col. 7, lines 32-34: biometric features utilized for cryptographic key generation) Bjorn does not specifically disclose whereby forming

uses said biometric information to form information that is independent of any absolute dimensions in an image representing said biometric information. However, Takhar discloses wherein forming uses said biometric information to form information that is independent of any absolute dimensions in an image representing said biometric information. (see Takhar col. 26, lines 7-24; col. 26, lines 38-41: ratios utilized for biometric parameter generation)

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Bjorn-Hillhouse without determining absolute dimensions e.g. Ratios as taught in Takhar. One would have been motivated to utilize relationship e.g. Ratios between those parts in order to analyze fingerprint information, so that the obtained information be translated into the cryptographic key to allow access with accurate verification and to optimize cryptographic key generation. (see Takhar col. 1, lines 46-53)

Regarding Claim 40, Bjorn discloses a system as in claim 38, wherein said routine forms said cryptographic key by identifying a reference on the fingerprint, and using location of features on the fingerprint to said reference to obtain said biometric information. (see Bjorn col. 3, lines 32-34; col. 4, lines 17-19; col. 7, lines 32-34: biometric features utilized for cryptographic key generation) Bjorn does not specifically disclose whereby a reference on the fingerprint, and using features relative to said reference to obtain said biometric information. However, Takhar discloses wherein a reference on the fingerprint, and using features on the fingerprint relative to said

reference to obtain said biometric information (see Takhar col. 26, lines 7-24; col. 26, lines 38-41: ratios (relative information) utilized for biometric parameter generation)

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Bjorn-Hillhouse without determining absolute dimensions e.g. Ratios as taught in Takhar. One would have been motivated to utilize relationship e.g. Ratios between those parts in order to analyze fingerprint information, so that the obtained information be translated into the cryptographic key to allow access with accurate verification and to optimize cryptographic key generation. (see Takhar col. 1, lines 46-53)

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kyung H Shin whose telephone number is (571) 272-3920. The examiner can normally be reached on 9 am - 7 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, David A Wiley can be reached on (571) 272-3923. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only.

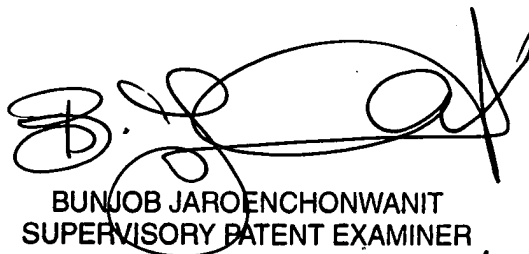
Application/Control Number:
09/577,449
Art Unit: 2143

Page 13

For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

K H S
Kyung H Shin
Patent Examiner
Art Unit 2143

KHS
December 26, 2007


BUNJOB JAROENCHONWANIT
SUPERVISORY PATENT EXAMINER
12/31/7